KEY EXCHANGE FOR A PROCESS-BASED SECURITY SYSTEM

ABSTRACT OF THE DISCLOSURE

A method and system for performing a key exchange between a client and a server having a process-based security system begins by sending user identification information from the client to the server. The server modifies the task structure of the client by the server to reflect a pending request for key exchange. The server generates a first random number and sends the first random number to the client. The server retrieves a password associated with the user identification information from storage. A user enters a password at the client. The server and the client then each calculate a first key using a transformative function operating on the password and the first random number. The client and server then use the result of the calculated first key as a first key. The server modifies the task structure of the client to reflect the completion of the key exchange.